"Putting Biometrics to Work for America"
Remarks by Bruce P. Mehlman
Assistant Secretary for Technology Policy,
United States Department of Commerce

Delivered February 14, 2002
at the Biometrics Consortium Conference
Arlington, Virginia

Thanks very much.

And thanks so much to the National Institute for Standards & Technology for hosting this outstanding and important conference.

For many years, we have looked to biometrics as a promising, emerging technology. That calculus has now changed. At this conference over the past three days we have learned that biometrics are no longer emerging - they're here. And September 11th taught us that biometrics are more than promising - they will be essential to our future security.
Eighteen days ago, in his State of the Union address, the President outlined the Administration's top three priorities:

- Winning the global war against terror;
- Securing citizens here at home; and
- Restoring American economic growth.

Technology - including biometrics - has an important role to play in helping us secure each of these goals. With respect to winning the war against terror, biometrics will be critical to our intelligence services, as they identify and track the enemies of freedom hiding around the world. Biometrics will also enable our fighting men and women - soldiers who are increasingly reliant upon information technologies and data communications - to communicate more securely and employ more effective perimeter defenses when based in hostile environments.

Biometrics are already being deployed to improve American security at home. From airports to nuclear power plants, from cyber security to building access technologies, biometrics will play a vital role in protecting our citizens and our way of life.

And biometrics have a role to play in restoring economic growth. Biometrics and good security practices can help reduce economic losses from terrorism and industrial espionage. Improved authentication, when combined with common-sense privacy practices, increase consumer confidence in conducting commerce online. And the biometrics industry itself represents a multi-billion dollar market, creating jobs in the United States and exports around the world.

* * * * *

Over the past 50 years, technology has played a critical role in improving America's economy and standard of living. Looking forward, technology is poised to assume an even greater role in our economy and our society. If innovation and new technologies profoundly *shaped* the 20th Century, they will *define* the 21st. But just as technological progress opens doors of possibilities, it also creates friction and challenges. New technologies often raise difficult legal, ethical and social policy questions. As the biometrics industry matures, it will be no exception.

Within the next 30 years, we expect everything may be connected to high-speed data networks - from household appliances to personal electronics to children's toys to clothes. Digital intelligence will recognize us, understand our needs, find us anywhere-anytime, and customize products and possibilities based upon our established preferences. But we'll need to consider how to cope with the changes this will bring and know when and how to set appropriate limits. For example,

- If you think Internet-based tracking and personalized marketing raises privacy questions, just wait. Face-recognition technologies may allow constant monitoring of citizens' movement and choices, without even the basic opt-in decision of going online. While this information would prove invaluable for marketers, merchants and news organizations, it begs the question of how much control citizens should have over information about their own movements once they leave their house.
- In the workplace, biometrics could help employers increase productivity, by tracking the movement of all human assets and identifying more efficient ways to conduct operations. How will this impact workplace morale and employee privacy?
- Biometrics could improve government processes such as voting, by reducing fraud and enforcing "one person one vote." But how would we ensure these technologies are universally understood, lest they deter participation in the political process by the least educated (who most fear technology and government)?
- In healthcare, fully deployed biometric databases could improve the speed and quality of care, minimizing errors and accidents (such as drug interactions in allergic patients). What rules should pertain to the security and protection afforded these most highly sensitive of databases?
- How do we best protect and empower consumers without litigating or regulating innovation into the ground? Where do we draw the line on information collection for commercial use - demanding notice? Offering opportunities to opt out? Requiring more?

Resolving these issues will not be easy. Indeed you may find that the biggest challenges for your industry are not in your laboratories, but rather in the hallowed halls of Congress. But getting it wrong could reduce innovation or imperil the very freedom we hope to enhance through this technology. So we'll need to get it right. And we'll need your help. As I turn to this afternoon's panel of experts, I'd urge everyone interested in the success of biometrics to remain engaged with policy makers - make your voices heard - and help us put biometrics to work for America.

Questions for expert panel:

- At what point should policy makers consider government rules to limit use of biometrics in the name of privacy?
- In addition to funding (through R&D and procurement) and the outstanding work of NIST (facilitating standards and technology development), how can the federal government best support biometric development and deployment?
- What policy barriers exist to your success in areas such as regulation, liability, market access, and federal procurement rules?
- Is biometric development and deployment being held back or advanced by the current pace of high-speed Internet access deployment, and how much bandwidth will be needed for biometric devices going forward?